




公告

您的一份力量，将为亿万用户保驾护航！

# 百度安全应急响应中心安全报告基本原则

公告类型：其他公告 发布时间：2024-05-08 20:45:50

1. 在漏洞测试过程中，须遵守渗透测试原则，严格遵守《网络安全法》的规定，对于上传 webshell、反弹 shell、搭建C2、内网扫描探测、恶意拖取数据、下载源码等越界行为以及危害业务正常运行行为，漏洞均 0 分处理，且百度有权利报案、举报、并配合刑事侦查机关提供相应证据。
2. 为了保护百度产品及业务的安全，降低用户安全风险，百度不允许任何未经BSRC同意的非法漏洞披露行为，若白帽私自将漏洞报告向外部发布或贩卖，BSRC有权减少或取消漏洞奖励且保留追究法律责任的权利。若有披露已修复漏洞的需求（如有参会议题等），请至少提前一周发邮件至security@baidu.com说明情况并保证漏洞报告敏感信息（域名、路由、账号密码、百度关键字以及logo等）均做打码处理，需确保无法辨识为百度产品，我们将评估该需求并且第一时间与你取得联系。
3. 不涉及安全问题的 Bug，包括但不仅限于产品功能缺陷、网页乱码、样式混乱、静态文件目录遍历、应用兼容性等问题请提交至 help.baidu.com。
4. 禁止使用社工手段，禁止以测试漏洞为借口，利用漏洞进行损害用户利益、影响业务运作、盗取用户数据等行为。如有违规，BSRC将采取进一步法律行动。
5. 漏洞标题描述需客观且符合报告内容，推荐以【产品线名称+漏洞核心影响】命名，漏洞相关字段需如实填写，禁止填写无意义的标签或文本。
6. 漏洞报告内容需明确漏洞触发点、完整复现步骤以及漏洞造成的实际危害，需确保漏洞能通过报告进行二次复现，请勿对漏洞危害进行猜测。
7. 百度员工请通过内部渠道报告漏洞。一旦发现内部员工使用外部账号通过 BSRC 提交漏洞，将把漏洞积分清零，并联系职业道德部门处理。

关于我们

百度安全应急响应中心（Baidu Security Response Center）是百度致力于维护互联网健康生态环境，保障百度产品和业务线的信息安全，促进安全专家的合作与交流而建立的漏洞收集及应急响应平台。本平台收集百度公司各产品线及业务上存在的安全漏洞，同时，我们也希望借此平台加强与业内各界的安全合作，共同打造简单可信赖的互联网健康生态。

快速入口

百度安全
隐私协议
联系我们
提交漏洞

关注我们


